ON THE QUADRATIC TWISTS OF
A FAMILY OF ELLIPTIC CURVES
(MATHEMATIKA 52(2005), NO. 1 – 2, 139 – 154)

GANG YU

Abstract. In this paper, we consider the average size of the 2-Selmer groups of a class of
quadratic twists of each elliptic curve over \( \mathbb{Q} \) with \( \mathbb{Q} \)-torsion group \( \mathbb{Z}_2 \times \mathbb{Z}_2 \). We prove the
existence of a positive proportion of quadratic twists of such a curve, each of which has rank 0 Mordell-Weil group.

1. Introduction

For an elliptic curve \( E \) over \( \mathbb{Q} \), by \( E(\mathbb{Q}) \) we denote its Mordell-Weil group. While
Mazur [9,10] has shown that the torsion part can be one of only finitely many possibilities,
ilittle is known for the rank. Nevertheless, it is generally believed that curves with large
ranks comprise a small “proportion” of all elliptic curves. In particular, it is conjectured
that “almost all” elliptic curves have rank 0 or 1. Moreover, Goldfeld [2] conjectured that
the average rank of the quadratic twists of any given elliptic curve over \( \mathbb{Q} \) is 1/2. A quick
consequence of this is that, for any elliptic curve over \( \mathbb{Q} \), asymptotically, there are at least half of the quadratic twists of this curve which have rank 0. Thus there is a comparatively weaker conjecture stating that, for any elliptic curve over \( \mathbb{Q} \), the rank 0 quadratic twists comprise a positive proportion of all quadratic twists of the given curve. In the general
case, this conjecture, though much weaker than the other famous ones related to elliptic
curves, is still open.

There have been numerous papers treating this problem for modular curves. Because
of the work of Kolyvagin[8], most of them are focusing on the non-vanishing of the \( L \)-
functions (see [6,7,11–14]). In light of the work of Shimura[15] and Waldspurger [17],
people have been able to get some partial results. With the knowledge about the Fourier
coefficients of some new forms, James [7] proved that the quadratic twists for some given
curve over \( \mathbb{Q} \) have rank 0 for a positive proportion of squarefree numbers. In [19], Wong

1991 Mathematics Subject Classification. 11G05, 14H52.
Key words and phrases. Elliptic Curves, 2-descent Procedure, Character Sums.

Typeset by \AMS-\TeX
proved that there is an infinite family of non-isomorphic elliptic curves such that for each curve a positive proportion of the quadratic twists have rank 0.

In a series of two papers [4,5], Heath-Brown studies the average order of the 2-Selmer groups of the congruent number curves $E_n : y^2 = x^3 - n^2 x$. As a byproduct of his main theorems, it is shown that a positive proportion of such curves have rank 0. In other words, a positive proportion of the quadratic twists of $E : y^2 = x^3 - x$ have rank 0. In this paper, we shall generalize this to all curves over $\mathbb{Q}$ with 2-torsion part $\mathbb{Z}_2 \times \mathbb{Z}_2$. Namely, we shall consider the curves $E = E(a,b)$ defined by the equation

$$y^2 = x(x+a)(x+b) \quad (1.1)$$

with $a, b \in \mathbb{Z}$ and $ab(a-b) \neq 0$. We shall prove that

**Theorem 1.** For the curve $E$ given by (1.1), a positive proportion of its quadratic twists have rank 0. Moreover, if assuming the parity conjecture of Mordell-Weil ranks, a positive proportion of its quadratic twists have rank 1.

One notes that, if not to pursue a quantitative version of Theorem 1 but just to prove the underlying proportional result qualitatively, one just needs to consider those $E$ with $(a,b) = 1$. Moreover, by a simple linear transformation, we can make $a$ even and $b$ odd and $ab > 0$. Note $E(-a,-b)$ gives a quadratic twist of $E(a,b)$, thus, for our purpose, it suffices to consider the curves

$$E(2a,b) : y^2 = x(x+2a)(x+b) \quad (1.2)$$

with $(2a,b) = 1$ and $a, b > 0$.

We shall derive the theorem (for curve $E(2a,b)$ given by (1.2)) by bounding the average size of the 2-Selmer groups of the quadratic twists $E_D$ with $D$ running over a subset of $\mathbb{N}$ of positive proportion. For convenience, throughout we shall assume $b > 2a > 0$ and $2 \nmid a$. From the forthcoming proof, one should be able to see that the first assumption does not lose generality and the second assumption, which makes the problem a little special, can be eliminated by considering the other case in exactly the same way. We shall not repeat the work for the case that $2 \mid a$.

Thus, we suppose that the curve $E = E(2a,b)$ satisfies $0 < 2a < b$, $(2a,b) = (2,a) = 1$, henceforth. For its quadratic twists

$$E_D : y^2 = x(x+2aD)(x+bD),$$

we shall let $D$ run over some special subset of $\mathbb{N}$.

Let $C$ be the conductor of $E$, so that $C$ is the product of the squarefree kernel of $ab(b-2a)$ and one of the numbers 8, 16 or 32. We shall consider those $D \in S(X; h)$, where
ON THE QUADRATIC TWISTS OF A FAMILY OF ELLIPTIC CURVES

\[ S(X; h) := \{ 1 \leq D \leq X : \mu^2(D) = 1, D \equiv h \mod C \}, \]

and \( h \) is a fixed integer coprime to \( C \). Here and throughout, \( \mu(\cdot) \) denote the Möbius function (and thus \( \mu^2(\cdot) \) is the character function of squarefree numbers).

Let \( c = b - 2a \). We describe several conditions, say \( Ca \), \( Cb \) and \(Cc\), as follows (where \( p \) denotes a prime):

(Ca): If \( p | a \) and \( \text{ord}_p(a) \) is even, then \( \left( \frac{bh}{p} \right) = -1 \),

(Cb): If \( p | b \) and \( \text{ord}_p(b) \) is even, then \( \left( \frac{2ah}{p} \right) = -1 \),

(Cc): If \( p | c \) and \( \text{ord}_p(c) \) is even, then \( \left( \frac{-bh}{p} \right) = -1 \).

Briefly, we denote by \( r(D) \) and \( s(D) \) the Mordell-Weil rank and 2-Selmer rank of \( E_D \), respectively. With a similar method as Heath-Brown [4] used for the congruent number curve, we are able to prove the following

**Theorem 2.** Let \( h \) be an integer coprime to \( C \) and satisfying the conditions \( (Ca) \), \( (Cb) \) and \( (Cc) \), then for the curve given by (1.2) we have

\[ \sum_{D \in S(X; h)} 2^s(D) = (3 + o(1)) \#S(X; h). \]

Combining Theorem 2 with the parity of \( s(D) \) proved by P. Monsky [11], we actually can prove a quantitative result for rank 0 quadratic twists of the curve given by (1.2).

**Theorem 1a.** For any integer \( d \), let \( \omega'(d) \) denote the number of primes \( p \) dividing \( d \) with \( \text{ord}_p(d) \) even. Then for the elliptic curve \( E \) given by equation (1.2), among all positive squarefree numbers, the proportion of those \( D \) with \( E_D \) having rank 0 is at least

\[ 2^{-\omega'(abc)-2} \frac{\varphi(C)}{3C}, \]

where \( \varphi(\bullet) \) is the Euler function.

Essentially the same proof gives a similar result about rank 1 quadratic twists. But in this case the corresponding result is conditional.

**Theorem 1b.** Let \( E \) satisfy the same conditions as in Theorem 1. Then, under the parity conjecture about the ranks of its quadratic twists, the proportion of squarefree quadratic twists that have rank 1 is at least
\[
2^{-\omega'(abc)-3} \frac{5\varphi(C)}{3C}.
\]

One notes that Theorems 1\(a\) and 1\(b\) obviously imply Theorem 1. Based on the result of Theorem 2, one can prove Theorems 1\(a\) and 1\(b\) in a similar way. Thus, for brevity, we shall only prove Theorems 1\(a\) and 2.

2. Proof of Theorem 1\(a\)

**Proof.** Recall that \(c = b - 2a\). From our conditions on \(a, b, c\) pairwise coprime and odd. Suppose

\[
a = p_1^{\alpha_1}...p_i^{\alpha_i}, \quad b = q_1^{\beta_1}...q_j^{\beta_j}, \quad c = l_1^{\gamma_1}...l_k^{\gamma_k}
\]

are the prime factorizations of \(a, b, c\), respectively. Then the conductor of \(E\) is given by

\[
C = 2^\mu p_1...p_i q_1...q_j l_1...l_k
\]

for some integer \(3 \leq \mu \leq 5\). According to Monsky [11], the parity of the 2-Selmer rank of \(E_D\) satisfies

\[
(-1)^{s(D)} = \omega_E,
\]

where \(\omega_E\) is the root number in the functional equation of \(L_E(s)\), if and only if \((\frac{-C}{D}) = 1\). Thus, if we choose \(D\) so that

\[
\left(\frac{-C}{D}\right) = \omega_E,
\]

then \(s(D)\) will be even. So, we will choose \(D\) in a residue class \(h \pmod{C}\) so that

\[
\omega_E = \left(\frac{-C}{D}\right) = \left(\frac{-C}{h}\right) = \left(\frac{-2^\mu p_1...l_k}{h}\right)
\]

which, with the law of quadratic reciprocity, is equivalent to

\[
(-1)^{\frac{h-1}{2} + \frac{(h-1)(p_1-1)...(l_k-1)}{4}} \left(\frac{2^\mu}{h}\right)^i \left(\frac{h}{p_i}\right)^{i'} \left(\frac{h}{q_j}\right)^{j'} \left(\frac{h}{l_{k'}}\right)^{k'} = \omega_E. \tag{2.3}
\]

From the fact that \(b - 2a = c\), and that \(a, b, c\) are all odd, we know \(a, b, c\) can not all be squares. Thus, on the left hand side of (2.3), there is at least one Jacobi symbol whose value is not determined by the conditions (Ca), (Cb) and (Cc). This implies that,
no matter what values $\omega_E(= \pm 1)$ and $p_1 \ldots l_k \pmod{4}$ take, there must be some $h \pmod{C}$ satisfying the conditions (Ca), (Cb) and (Cc) and the parity condition (2.3). Furthermore, it is not hard to see that we have exactly $2^\omega(abc) - 2\varphi(C)$ odd congruence classes modulo $C$ satisfying conditions (Ca), (Cb), (Cc) and (2.3). (The conditions (Ca), (Cb), (Cc) account for the factor $2^\omega(abc)$, the fact that $h$ is odd accounts for a factor $2^{-1}$, and that fact that $h$ satisfies (2.3) accounts for the last factor $2^{-1}$.)

Now for a fixed $h$ satisfying (Ca), (Cb), (Cc) and condition (2.2), from the facts that

$$\sum_{D \in S(X; h)} s(D) = (3 + o(1))\#S(X; h), \quad (2.4)$$

and that $s(D)$ is even, we conclude that, asymptotically, at least $1/3$ of the elements $D$ of $S(X; h)$ satisfy $s(D) = 0$. Note $r(D) \leq s(D)$, we thus conclude that, asymptotically, at least $1/3$ of the $E_D$ with $D \in S(X; h)$ have rank 0. Since for different $h_1$, $h_2$ coprime to $C$ we have $\#S(X; h_1) \sim \#S(X; h_2)$ as $X \to \infty$, we have completed the proof. \hfill $\square$

3. Order of the 2-Selmer group

We apply a similar discussion as Heath-Brown does in [4]. For each squarefree $D$, the four 2-torsion points

$$\vartheta, \quad (0, 0), \quad (-2aD, 0), \quad (-bD, 0)$$

comprise a subgroup $\mathbb{Z}_2 \times \mathbb{Z}_2$ of the torsion part of $E_D(\mathbb{Q})$, call it $E_D(\mathbb{Q})_{2-tors}$.

For any non-torsion point $P := (x, y) \in E_D(\mathbb{Q})$, the coset in $P + E_D(\mathbb{Q})_{2-tors}$ consists of

$$(x, y), \quad \left(\frac{2abD^2}{x}, *, *, *, x \to \infty\right), \quad \left(-2aD(x + bD)\frac{x + 2aD}{x}, x + bD, x \to \infty\right)$$

which contains exactly one $(x', y')$ with $x' > 0$ and $|x'|_2 < 1$. If choosing this one as the representative of $P + E_D(\mathbb{Q})_{2-tors}$, we have a canonical map

$$\theta: \frac{E_D(\mathbb{Q})}{E_D(\mathbb{Q})_{2-tors}} \to G \times G \times G, \quad \text{where} \quad G := \frac{\mathbb{Q}^\times}{\mathbb{Q}^\times_2},$$

$$(x', y') \mapsto (x', x' + 2aD, x' + bD) \pmod{\mathbb{Q}^\times_2}.$$

Further, the image of $\theta$ has size $2^{r(D)}$. 
Now, suppose \((2rt^{-2}, st^{-3})\) is the representative of \(P\) satisfying \((rs, t) = 1, r > 0, 2 \nmid t\). Then

\[s^2 = 2r(2r + 2aDt^2)(2r + bDt^2)\].

Suppose \((r, D) = D_0\) and write \(r = r'D_0\). Then

\[s^2 = 4D_0^3r'(r' + \frac{aD}{D_0}t^2)(2r' + \frac{bD}{D_0}t^2)\]

so that

\[D_0\left(\frac{s}{2D_0^2}\right)^2 = r'(r' + \frac{aD}{D_0}t^2)(2r' + \frac{bD}{D_0}t^2)\]

by noticing \(D_0^2 | s\) since \(D_0\) is squarefree.

Suppose

\[\left(r', r' + \frac{aD}{D_0}t^2\right) = (r', a) := u, \quad \text{say,}\]

\[\left(r', 2r' + \frac{bD}{D_0}t^2\right) = (r', b) := v, \quad \text{say,}\]

and

\[\left(r' + \frac{aD}{D_0}t^2, 2r' + \frac{bD}{D_0}t^2\right) = \left(b - 2a, r' + \frac{aD}{D_0}t^2\right) := w, \quad \text{say.}\]

Obviously \(u, v, w\) are coprime in pairs, \(2 \nmid uvw\) and, since we are considering things mod\(\mathbb{Q} \times 2\), we may assume that \(uvw\) is squarefree. Then we have

\[r' = uvD_1V^2,\]

\[r' + \frac{aD}{D_0}t^2 = uvD_2Y^2,\]

\[2r' + \frac{bD}{D_0}t^2 = uvD_3Z^2,\]

where \(D_1D_2D_3 = D_0\). Writing \(\frac{D}{D_0} = D_4, a = a'u, b = b'v\) and \(c = b - 2a = c'w\), we have the following system of quadratic equations:
\[
\begin{align*}
    vD_1V^2 + a'D_4W^2 &= wD_2Y^2 \\
    2uD_1V^2 + b'D_4W^2 &= wD_3Z^2.
\end{align*}
\] (3.1)

As with \(u, v, w\), we can absorb square divisors of \(a', b', c'\) into the variables \(V, W, Y, Z\), so we assume now that \(a', b', c'\) are squarefree. From the definition of Selmer group for an elliptic curve, the number of systems (3.1) which are everywhere locally solvable equals \(2^{s(D)}\), the order of the 2-Selmer group modulo the 2-torsion group. Note that if a prime \(p\) does not divide any of the coefficients of the system, then the system is solvable in \(\mathbb{Q}_p - \{0\}\). So it suffices to just consider the primes \(p|abcD\).

We start the prime division discussion as follows:

**P1.** If \(p|D_1\), then we need \(\left(\frac{a'wD_2D_4}{p}\right) = \left(\frac{b'wD_3D_4}{p}\right) = 1\),

**P2.** If \(p|D_2\), then we need \(\left(\frac{-a'vD_1D_4}{p}\right) = \left(\frac{c'vD_3D_4}{p}\right) = 1\),

**P3.** If \(p|D_3\), then we need \(\left(\frac{-2b'uD_1D_4}{p}\right) = \left(\frac{-2c'uD_2D_4}{p}\right) = 1\),

**P4.** If \(p|D_4\), then we need \(\left(\frac{vwD_1D_2}{p}\right) = \left(\frac{2uwD_1D_3}{p}\right) = 1\).

Before we present the prime division discussion about \(a', b', c'\) and \(u, v, w\), we explain why we have restricted \(h\) to satisfying conditions (Ca), (Cb) and (Cc). The purpose of choosing \(h\) in this way is to ensure that if the system (3.1) is \(\mathbb{Q}_p\)-solvable for all \(p\), then \((a', u) = (b', v) = (c', w) = 1\). For example, if there were some prime \(p\) dividing \((a', u)\) for a \(\mathbb{Q}_p\)-solvable system (3.1), then we know \(\text{ord}_p(a)\) must be even and thus (Ca) holds in this case, and from (3.1) we have

\[
\left(\frac{vwD_1D_2}{p}\right) = \left(\frac{b'wD_3D_4}{p}\right) = 1
\]

which implies

\[
\left(\frac{bD_1D_2D_3D_4}{p}\right) = \left(\frac{bD}{p}\right) = \left(\frac{bh}{p}\right) = 1,
\]

contradictory to restriction (Ca). Thus, we may assume that \(a'b'c'uvw\) is squarefree. So, now for any \(\mathbb{Q}_p\)-solvable system (3.1), we have

**P5.** If \(p|a'\), then \(\left(\frac{vwD_1D_2}{p}\right) = 1\),
P6. If \( p|b' \), then \( \left( \frac{2uwD_1D_2}{p} \right) = 1 \),

P7. If \( p|c' \), then \( \left( \frac{2uvD_2D_1}{p} \right) = 1 \),

P8. If \( p|u \), then \( \left( \frac{b'wD_3D_4}{p} \right) = 1 \),

P9. If \( p|v \), then \( \left( \frac{a'wD_2D_4}{p} \right) = 1 \),

P10. If \( p|w \), then \( \left( \frac{-a'vD_1D_4}{p} \right) = 1 \).

In view of the prime division discussions, if, for example, \( p|D_1 \), then we need

\[
\frac{1}{4} \left\{ 1 + \left( \frac{a'wD_2D_4}{p} \right) \right\} \left\{ 1 + \left( \frac{b'wD_3D_4}{p} \right) \right\} = 1,
\]

namely,

\[
\frac{1}{4} \left\{ 1 + \left( \frac{a'wD_2D_4}{p} \right) + \left( \frac{b'wD_3D_4}{p} \right) + \left( \frac{a'b'D_2D_3}{p} \right) \right\} = 1. \tag{3.2}
\]

By taking the product of (3.2) over all the prime factors \( p \) of \( D_1 \), with the same notation as Heath-Brown’s, we denote

\[
\Pi(D_1) := \prod_{p|D_1} \frac{1}{4} \left\{ 1 + \left( \frac{a'wD_2D_4}{p} \right) + \left( \frac{b'wD_3D_4}{p} \right) + \left( \frac{a'b'D_2D_3}{p} \right) \right\} = 4^{-\omega(D_1)} \sum_{D_1=D_{10}D_{12}D_{13}D_{14}} \left( \frac{a'wD_2D_4}{D_{13}} \right) \left( \frac{b'wD_3D_4}{D_{12}} \right) \left( \frac{a'b'D_2D_3}{D_{14}} \right), \tag{3.3}
\]

and we can similarly denote \( \Pi(D_2), \Pi(D_3) \) and \( \Pi(D_4) \) according to conditions P2, P3 and P4. We also denote

\[
\Pi(u) := 2^{-\omega(u)} \sum_{u_s|u} \left( \frac{b'wD_3D_4}{u_s} \right), \tag{3.4}
\]

where \( \omega(u) \) is the number of different prime factors of \( u \). And similarly define \( \Pi(v), \Pi(w), \Pi(a') \Pi(b') \) and \( \Pi(c') \) in accordance with the conditions P5-P10.

From the above discussion, it is then easy to verify the following lemma, though the formula (3.8) looks very complicated.
Lemma 1. We have

\[ 2s(D) = \sum_{\vec{D}} \sum_{\vec{a}} \sum_{\vec{b}} \sum_{\vec{c}} \Pi(D_1) \Pi(D_4) \Pi(u) \Pi(c') \quad (3.5) \]

where the sum is taken over all the factorizations

\[ D = D_1 D_2 D_3 D_4, \quad \gamma(a) = a'u, \quad \gamma(b) = a'v \quad \text{and} \quad \gamma(c) = c'w, \]

where \( \gamma(m) \) is \( m \) divided by its largest square divisor.

We may further write this out as

\[ 2s(D) = \sum_{\vec{D}} g(\vec{D}), \quad (3.6) \]

where the sum is taken over all the factorizations of

\[ D = \prod_{1 \leq i \leq 4} \prod_{0 \leq j \neq i \leq 4} D_{ij} \]

and where, with \( \star \) briefly representing the letters \( a', b', c', u, v, w \) and the \( a'_s, b'_s, c'_s, u_s, v_s, w_s \)

\[ g(\vec{D}) = \sum_{\gamma(a)=a'u} \sum_{\gamma(b)=b'v} \sum_{\gamma(c)=c'w} \sum_{u} \sum_{v} \sum_{w} \sum_{a'_{s}} \sum_{b'_{s}} \sum_{c'_{s}} g_{\star}(\vec{D}) \quad (3.7) \]

with

\[ g_{\star}(\vec{D}) = 2^{-\omega(abc)} \left( \frac{-1}{\alpha} \right) \left( \frac{2}{\beta} \right) \prod_{i=1}^{4} 4^{-\omega(D_{i0})} \prod_{j \neq 0, i} 4^{-\omega(D_{ij})} \prod_{k \neq i, j} 4^{-\omega(D_{ij})} \prod_{0 \leq k \neq l \leq 4} \left( \frac{D_{kl}}{D_{ij}} \right) \]

\[ \times \left( \frac{a'}{D_{13} D_{14} D_{23} D_{24} v_s w_s} \right) \left( \frac{b'}{D_{12} D_{14} D_{32} D_{34} u_s} \right) \left( \frac{c'}{D_{21} D_{24} D_{31} D_{34}} \right) \]

\[ \times \left( \frac{u}{D_{31} D_{32} D_{41} D_{42} b'_s c'_s} \right) \left( \frac{v}{D_{21} D_{23} D_{41} D_{43} w_s a'_s c'_s} \right) \left( \frac{w}{D_{12} D_{13} D_{42} D_{43} u_s v_s a'_s b'_s} \right) \]

\[ \times \prod_{j \neq 1} \left( \frac{D_{1j}}{a'_s b'_s w_s} \right) \prod_{j \neq 2} \left( \frac{D_{2j}}{a'_s c'_s v_s} \right) \prod_{j \neq 3} \left( \frac{D_{3j}}{b'_s c'_s u_s} \right) \prod_{j \neq 4} \left( \frac{D_{4j}}{u_s v_s w_s} \right), \quad (3.8) \]
where
\[
\alpha = D_{23}D_{24}D_{31}D_{32}w_s \quad \text{and} \quad \beta = D_{31}D_{32}D_{41}D_{42}b'_s c'_s.
\]

4. Some Error Cases

With the expression in lemma 1, the sum \(\sum 2^{s(D)}\) is translated into a multiple character sum with 28 new variables, 12 of which are divisors of \(a, b\) and \(c\) of some special types and the other 16 variables \(D_{ij}\) are subject to the conditions that each \(D_{ij}\) is squarefree, that they are pairwise coprime and that their product \(D\) satisfies

\[D \leq X, \quad D \equiv h \mod C.\]

The main contribution to the asymptotic formula of \(\sum 2^{s(D)}\) raises from the terms with \(D\) and \(abc\) having several special types of factorizations that will be specified in the last section. We divide the range of each \(D_{ij}\) into intervals \([A_{ij}, 2A_{ij}]\) with \(A_{ij}\) running over powers of 2 and

\[1 \ll \prod A_{ij} \ll X\]

This gives us \(O(\log^{16} X)\) non-empty subsums, each written as \(S(\vec{A})\), \(\vec{A}\) referring to the 16-tuple of numbers \(A_{ij}\). Further, we shall with a brief notation \(S_*(\vec{A})\) define the sum of \(g_*(\vec{D})\) with the \(D_{ij}\)'s running over the \(A_{ij}\)'s.

With Heath-Brown’s terminology, two variables ♣ and ♠ are called “linked” if exactly one of the Jacobi symbols

\[
\left(\frac{\♣}{\♠}\right) \quad \text{or} \quad \left(\frac{\♠}{\♣}\right)
\]

occurs in \(g(\vec{D})\). In the case that we have ♣ = \(D_{ij}\) and ♠ = \(D_{kl}\) for some variables \(D_{ij} \neq D_{kl}\), it is clear that they are linked if and only if \(i \neq k\) and precisely one of the conditions \(l \neq 0, j \) or \(j \neq 0, k\) holds.

Two unlinked variables \(D_{ij}\) and \(D_{kl}\) are called “joined” if both Jacobi symbols

\[
\left(\frac{D_{ij}}{D_{kl}}\right) \quad \text{and} \quad \left(\frac{D_{kl}}{D_{ij}}\right)
\]

occur in the expression of \(g(\vec{D})\), otherwise they are called “independent”.

Before giving estimates to some error cases, we state two lemmas concerning estimating character sums here. The first one is Lemma 6 of [4] and the second is Lemma 4.1 of [20].
Lemma 2. Let $N$ be sufficiently large. Then for arbitrary positive integers $q$, $r$ and any non-principal character $\chi \pmod{q}$, we have

$$\sum_{n \leq x, (n,r) = 1} \mu^2(n)4^{-\omega(n)}\chi(n) \ll xd(r) \exp(-\eta \sqrt{\log x})$$  \hspace{1cm} (4.1)$$

with a positive constant $\eta = \eta_N$, uniformly for $q \leq \log^N x$. Here and throughout $d(r)$ denotes the usual divisor function.

Lemma 3. Suppose $\epsilon > 0$ is any fixed number, $X$, $M$ and $N$ are sufficiently large real numbers, and $\{a_m\}$ and $\{b_n\}$ are two complex sequences, supported on odd integers, satisfying $|a_m|$, $|b_n| \leq 1$. Fix positive integers $h$, $q$ satisfying $(h, q) = 1$ and $q \leq \{\min(M, N)\}^{\epsilon/3}$. Let

$$S := \sum_{m,n} a_m b_n \left(\frac{m}{n}\right),$$

where the summation is subject to

$$M < m \leq 2M, \quad N < n \leq 2N, \quad mn \leq X \quad \text{and} \quad mn \equiv h \pmod{q}.$$ 

Then we have

$$S \ll MN^{\frac{15}{16}} + \epsilon + M^{\frac{15}{16}} + \epsilon N,$$ \hspace{1cm} (4.2)$$

where the constant involved in the $\ll$-symbol depends on $\epsilon$ only.

Henceforth, We set

$$T := \exp((\log X)^{\frac{1}{20}}) \quad \text{and} \quad K := (\log X)^{340}. \hspace{1cm} (4.3)$$

Now we consider some subsums of $\sum 2^\omega(D)$ in the following several cases.

- Case 1: $A_{ij}, A_{kl} > K$, where $D_{ij}$ and $D_{kl}$ are linked.

First we note that, from Lemma 1, $g_*(\bar{D})$ can be written in the form

$$g_*(\bar{D}) = \left(\frac{D_{ij}}{D_{kl}}\right) \lambda(D_{ij})\xi(D_{kl})\zeta,$$ \hspace{1cm} (4.4)$$

where the function $\lambda(D_{ij})$ is the product of $4^{-\omega(D_{ij})}$ and the Jacobi symbols appearing in (3.8) that contain $D_{ij}$ (other than $(\frac{D_{ij}}{D_{kl}})$), and similarly for $\xi(D_{kl})$, and $\zeta$ is the product of $2^{-\omega(abc)}$, $4^{-\omega(D/D_{ij}D_{kl})}$ and the other Jacobi symbols left. It’s clear that $|\lambda(D_{ij})|, |\xi(D_{kl})|, |\zeta| \leq 1$.

Let $S(\bar{A})$ be with $A_{ij}, A_{kl} > K$. From (4.4), we have
\[ S(\tilde{A}) \ll \max_{\lambda, \xi} \sum_{A_{rs} < D_{rs} \leq 2A_{rs}} | \sum_{D_{ij}, D_{kl}} \left( \frac{D_{ij}}{D_{kl}} \right) \lambda(D_{ij}) \xi(D_{kl}) |, \]  

where the maximum is actually taken with respect to the factorizations of \( abc \) which affect the values of \( \lambda(D_{ij}) \) and \( \xi(D_{kl}) \). We can take \( \epsilon \) arbitrarily small in Lemma 3 when \( X \) is sufficiently large. In particular, we have

\[ S(\tilde{A}) \ll \sum_{A_{rs} < D_{rs} \leq 2A_{rs}} A_{ij} A_{kl} K^{-\frac{1}{20}} \ll \left( \prod A_{ij} \right) K^{-\frac{1}{20}} \ll X(\log X)^{-17}. \]  

In view of this, we conclude that the subsum of \( \sum 2^s(D) \) with two linked variables \( D_{ij}, D_{kl} > K \) is bounded by

\[ \sum' X(\log X)^{-17} \ll (\log X)^{4800} \cdot X(\log X)^{-17} \ll X(\log X)^{-1}. \]  

Here and throughout the head-script “\( \tilde{\cdot} \)” indicates that the sum is subject the prescribed restrictions.

• Case 2: \( A_{ij} > T \), and \( A_{kl} \leq K \) for all \( D_{kl} \) linked with \( D_{ij} \) and the product of the \( D_{kl} \)’s is not 1.

We write \( D' \) as the product of all \( D_{kl} \) linked with \( D_{ij} \), then trivially \( D' \ll (\log X)^{4800} \). Applying the law of quadratic reciprocity to the “joined” pairs of Jacobi symbols involving \( D_{ij} \), we can write \( g_*(\tilde{D}) \) in the form

\[ g_*(\tilde{D}) = 4^{-\omega(D_{ij})} \left( \frac{D_{ij}}{D'} \right) \chi(D_{ij}) \zeta, \]  

where \( \chi \) is a character modulo \( C \) arising from the product of the Jacobi symbols involving \( D_{ij} \) and the factors of \( abc \) and a modulo 4 character from the application of quadratic reciprocity, and \( \zeta \) is the product of \( 2^{-\omega(abcd)} \), \( 4^{-\omega(D/D_{ij})} \) and the other Jacobi symbols left. It is obvious that \( |\zeta| \leq 1 \) and \( \zeta \) doesn’t depend on \( D_{ij} \). Thus we have

\[ S(\tilde{A}) \leq \sum_{\tilde{a}, \tilde{b}, \tilde{c}} |S_*(\tilde{A})| \leq \sum_{\tilde{a}, \tilde{b}, \tilde{c}} \sum_{D_{ij}} \left| \sum_{D_{rs}} \mu^2(D_{ij}) 4^{-\omega(D_{ij})} \left( \frac{D_{ij}}{D'} \right) \chi(D_{ij}) \right|, \]  

where the notation \( \tilde{a}, \tilde{b} \) and \( \tilde{c} \) indicate that the summation is over factorizations of \( abc \) as shown in (3.7), where the inner sum is also subject to that \( D_{ij} \) is coprime to all the other variables \( D_{rs} \) and

\[ D_{ij} \equiv h \bar{k} \pmod{C}, \]
where \( \bar{n} \) defines the multiplicative inverse of \( n \) with respect to the given modulo, and \( k \) is the product of all other \( D_{rs} \) modulo \( C \). This last restriction can be removed by introducing the characters modulo \( C \) into play. Noticing that \( \chi \) in (4.9) is also of modulo \( C \), we have

\[
S(\bar{A}) \ll \sum_{\chi \pmod{C}} \sum_{(r,s) \neq (i,j)} \left| \sum_{D_{ij}} \mu^2(D_{ij})4^{-\omega(D_{ij})} \left( \frac{D_{ij}}{D^r} \right) \chi(D_{ij}) \right|,
\]

where the constant involved in the \( \ll \)-symbol depends on \( C \) only.

In the case that \( D' \neq 1 \), Lemma 2 implies that

\[
S(\bar{A}) \ll A_{ij} \exp(-\eta \sqrt{A_{ij}}) \prod_{(r,s) \neq (i,j)} \left( \sum_{D_{rs}} d(D_{rs}) \right) \ll X \exp(-\eta \sqrt{A_{ij}})(\log X)^{15}.
\]

This implies that, in this case,

\[
\sum_{\bar{A}} |S(\bar{A})| \ll X(\log X)^{-1}, \tag{4.10}
\]

\( \bullet \) Case 3: \( A_{ij} > T \) for at most three variables \( D_{ij} \).

Write \( m \) as the product of the \( D_{ij} \)'s with \( A_{ij} \leq T \) and \( n \) as the product of the \( D_{ij} \)'s with \( A_{ij} > T \). Trivially, each \( m \) can arise at most \( 16^{\omega(m)} \) times and each \( n \) can arise at most \((16)3^{\omega(n)}\) times. For any fixed \( \gamma > 0 \), it is well known that

\[
\sum_{n \leq N} \gamma^{\omega(n)} \ll N(\log N)^{\gamma-1}
\]

holds for every \( N \geq 3 \). Thus,

\[
\sum_{A_{ij}}' |S(\bar{A})| \ll \sum_{m \leq T^{16}} 4^{\omega(m)} \sum_{n \leq X/m} \left( \frac{3}{4} \right)^{\omega(n)} \ll \sum_{m \leq T^{16}} 4^{\omega(m)} \frac{X}{m} \left( \log \frac{X}{m} \right)^{-\frac{3}{4}}
\]

\[
\ll \frac{X}{(\log X)^{\frac{3}{4}}} \sum_{m \leq T^{16}} \frac{4^{\omega(m)}}{m} \ll \frac{X}{(\log X)^{\frac{3}{4}}} \cdot (\log T)^4 \ll X(\log X)^{-\frac{1}{2}}. \tag{4.11}
\]

In addition to the subsums considered above, some \( S_{*}(\bar{A}) \) obviously give negligible contribution. If \( A_{ij} > T \) and \( D_{ij} \) is linked with some nontrivial divisor of \( abc \), then with the argument given in the second case, we have

\[
\sum_{A_{ij}}' |S_{*}(\bar{A})| \ll X(\log X)^{-1}. \tag{4.12}
\]

Collecting the estimates (4.7), (4.10), (4.11) and (4.12) together, we have the following lemma.
Lemma 4. We have

\[ \sum' |S(\vec{A})| \ll X(\log X)^{-\frac{1}{20}}, \]  

(4.13)

where the sum over \( \vec{A} \) is for all sets in which either there are at most three \( A_{ij} \geq T \), or there are linked variables \( D_{ij} \) and \( D_{kl} \) with \( A_{ij} \geq T \) and \( D_{kl} > 1 \).

Furthermore, we have

\[ \sum' |S_*(\vec{A})| \ll X(\log X)^{-1}, \]  

(4.14)

where the sum over \( \vec{A} \) is for there is \( A_{ij} \geq T \) with \( D_{ij} \) linked with a nontrivial factor of abc.

5. More Error Cases

From Lemma 4, we see that the main terms arise from the cases that at least four of the \( D_{ij} \)'s are with \( A_{ij} \geq T \), and no two of them are linked, and every variable \( D_{kl} \) linked to any one of these \( D_{ij} \)'s must be 1. Before distinguishing some of these cases which still give negligible contributions from the others which the main term arises from, first we want to identify the cases that are not included in the estimate (4.13).

To take an example, let’s say \( A_{12}, A_{21} > T \), then we have

\[ D_{30} = D_{31} = D_{32} = D_{40} = D_{41} = D_{42} = D_{23} = D_{24} = D_{13} = D_{14} = 1, \]

since these variables are either linked with \( D_{12} \) or \( D_{21} \), or both. Thus, among \( A_{10}, A_{20}, A_{34} \) and \( A_{43} \), two or more must be greater than \( T \). If assuming \( A_{10} > T \), then we must have \( D_{34} = D_{13} = 1 \) since they are linked with \( D_{10} \); similarly, if \( A_{34} > T \), then we have \( D_{10} = D_{20} = 1 \) since these variables are linked with \( D_{34} \). This yields that, if \( A_{12}, A_{21} > T \), then we have either

\[ A_{12}, A_{21}, A_{10}, A_{20} > T \] and all other variables \( D_{ij} = 1 \),

or

\[ A_{12}, A_{21}, A_{34}, A_{43} > T \] and all other variables \( D_{ij} = 1 \).

We note that the cases excluded by Lemma 4 are the same as those excluded by Lemma 8 in [4]. With a case by case discussion, Heath-Brown[4] actually shows that each of the the left cases not included in Lemma 4 is with exactly 4 non-trivial \( D_{ij} \)'s. Moreover, the indices of the four variables with a range greater than \( T \) are given by

\[ 10, 20, 30, 40, \quad i0, j0, ij, ji, \quad i0, ij, ik, il, \]

\[ i0, ji, ki, li, \quad ij, ik, lj, lk, \quad ij, ji, kl, lk, \quad (5.1) \]
where \( i, j, k \) and \( l \) are distinct non-zero indices, and in each case all the other variables \( D_{ij} \) are 1. As a reminder, in every case listed, no two variables are linked.

For each one of these cases, by re-labelling the variables, we may write \( S(\vec{A}) \) in the form

\[
\sum_{\gamma(a)=a'w} \sum_{\gamma(b)=b'v} \sum_{\gamma(c)=c'w} \sum_{\gamma(d)=d'v} \chi_1(n_1)\chi_2(n_2)\chi_3(n_3)\chi_4(n_4)PQ,
\]

(5.2)

where \( Q = 4^{-\omega(n_1n_2n_3n_4)} \) and \( P \) comes from the product of \( 2^{-\omega(abc)} \) and some terms \( \pm 1 \) from applying the law of quadratic reciprocity, and \( \chi_i \)'s are the characters modulo 8, arising from \( (\frac{-1}{\alpha}) \) and \( (\frac{2}{\beta}) \) in the expression of \( g(D) \).

It’s very nice that in each case, at least two variables are independent, so we can reduce (5.2) to

\[
\sum_{n_3,n_4} \sum_{n_3} \sum_{n_4} \sum \chi_3(n_3)\chi_4(n_4)PQ,
\]

(5.3)

where \( n_3 \) and \( n_4 \) are assumed to be independent and \( P \) can be written as the product of \( 2^{-\omega(abc)} \) and characters \( \psi_3(n_3), \psi_4(n_4) \) modulo 4, depending on the other variables alone. So we need to estimate sums of the form

\[
\sum_{n_3} \sum_{n_4} (\psi_3 \chi_3)(n_3)(\psi_4 \chi_4)(n_4)\mu^2(n_3)\mu^2(n_4)4^{-\omega(n_3)}4^{-\omega(n_4)},
\]

(5.4)

where \( n_3 \) and \( n_4 \) are respectively running over some large intervals, satisfying \( (n_3, n_4) = 1 \) and \( n_3n_4 \) congruent to some fixed number modulo \( C \).

To give a non-trivial estimate for (5.4) when either \( \psi_3 \chi_3 \) or \( \psi_4 \chi_4 \) is non-principal, we appeal to the following result.

**Lemma 5.** Let \( X > 0 \) and \( M, N \geq T > 0 \) be given. Then for any positive integer \( r \), any odd integer \( h \), and any distinct characters \( \chi_1, \chi_2 \pmod{8} \), we have

\[
\sum_{m,n} \mu^2(m)\mu^2(n)4^{-\omega(m)-\omega(n)}\chi_1(m)\chi_2(n) \ll d(r)X \exp(-\eta\sqrt{\log T}) \log X
\]

(5.5)

for some positive absolute constant \( \eta \), where the sum is over coprime variables satisfying the conditions

\[
M < m \leq 2M, \quad N < n \leq 2N, \quad mn \leq X, \quad mn \equiv h \pmod{C}, \quad (mn,r) = 1.
\]
Proof. This is just a little bit different from lemma 10 of [3], where \( mn \) is running over an arithmetic progression modulo 8. We can easily get estimate (5.5) from lemma 2 by noticing that in this case at least one of the characters \( \chi_1, \chi_2 \) is non-principal. □

We write \( A_{ij} \) as \( A_3 \) if \( n_3 \) comes from \( n_{ij} \), similarly for \( A_4 \). In the case \( A_3, A_4 \geq T \), if some character attached to \( n_3 \) or \( n_4 \), say \( \psi_3 \chi_3 \), is non-trivial, then by using lemma 3, one gets an upper bound for the above sum, which leads to an upper bound for \( S(\bar{A}) \) acceptable in the error term of Theorem 2.

We claim that, except for the four cases with the following indices

\[
(10, 20, 30, 40); \quad (10, 12, 13, 14); \quad (30, 13, 23, 43); \quad (40, 14, 24, 34),
\]

we can choose the labelling properly so that at least one of \( \psi_3 \chi_3 \) and \( \psi_4 \chi_4 \) is non-trivial. Sometimes we may achieve this by finding \( \psi_3 = \psi_4 \) while \( \chi_3 \neq \chi_4 \), or, under the assumptions made at the beginning of this section, we can show that some cases other than those in (5.6) do not happen.

I. \( i0, j0, ij, ji \)

In four of the six cases, it is not difficult to find out the \( n_3 \) and \( n_4 \) that we need. Except \( (i, j) = (1, 2) \) or \( (3, 4) \), at least one of \( D_{ij} \) and \( D_{ji} \) corresponds to a non-trivial character. Since any pair of variables is independent, if \( \chi_{ij} \neq \chi_0 \), then by taking

\[
D_{ij} = D_{i0}, \quad D_{ji} = D_{ij},
\]

we have \( \psi_3 = \psi_4 \) and \( \chi_3 = \chi_0 \neq \chi_4 \). When \( (i, j) = (1, 2) \) or \( (3, 4) \), things become interesting. For example, if \( i = 1, j = 2 \), then in this case, except \( \Pi(D_1), \Pi(D_2), \Pi(u) \), all the factors in (3.5) are trivially 1. Since \( a'_s, b'_s, c'_s, v_s \) and \( w_s \) have to be 1 because of (4.14), and \( b'w, c'v \) are respectively linked with \( D_{12}, D_{21} \), again from (4.14), we just need consider the case \( b'w = c'v = 1 \), which implies \( b = c = 1 \). (Recall that this actually means \( b \equiv c \equiv 1 \pmod{\mathbb{Q}^\times} \), i.e., both \( b \) and \( c \) are squares.) But this is absurd because

\[
b - c = 2a \equiv 2 \pmod{4}
\]

The same contradiction arises in the case \( (i, j) = (3, 4) \).

II. \( ij, ji, kl, lk \)

In the case \( (i, j) \neq (1, 2) \) and \( (3, 4) \), we may take \( n_3 = D_{ij} \) and \( n_4 = D_{ji} \), and it turns out that the characters attached to \( n_3 \) and \( n_4 \) are different. The interesting case is \( (i, j) = (1, 2) \) or \( (3, 4) \). Assume \( i = 1, j = 2 \). Because of lemma 2, it suffices to consider the case that \( b'_s = b', w_s = w, c'_s = c' \) and \( v_s = v \). We take \( n_3 = D_{12}, n_4 = D_{21}, \) then \( \psi_3 = \psi_4 \) because both \( n_3 \) and \( n_4 \) are joined with \( D_{34} \) and \( D_{43} \). If there were \( \chi_3 \neq \chi_4 \), then we must have
because of the law of quadratic reciprocity, which implies that
\[ 2a = b - c \equiv 0 \pmod{4} \]
contradictory to the fact that \( 2 \nmid a \).

III. \( ij, ik, lj, lk \)

Among all of these, except for cases (13, 14, 23, 24) and (31, 32, 41, 42), it can be seen that, if taking \( n_3 = D_{ij}, n_4 = D_{ik} \) with \( i \neq 1 \), then the characters attached to \( n_3, n_4 \) are different. In the case we have (31, 32, 41, 42), because of (4.14), we just need consider cases where \( b' = c' = 1, u_s = u, v = w = 1 \), which again implies that \( b = c = 1 \), leading to contradiction. In the case (13, 14, 23, 24), we have the same conclusion.

IV. \( i0, ij, ik, il \)

If \( i \neq 1 \), then things are almost trivial, since one can choose \( n_3 = D_{i0} \) and easily take \( n_4 \) to be some other variable so that the characters attached to \( n_3 \) and \( n_4 \) are different.

V. \( i0, ji, ki, li \)

These two cases are not in the same category as the above, but the criterion is the same. When \( i = 1 \) or 2, there is at least one variable, \( ji \), say, with associated character \( \left( \frac{2}{z} \right) \). We may then take
\[ n_3 = D_{i0}, \quad n_4 = D_{ij}. \]
(Note \( n_3 \) and \( n_4 \) are independent).

6. Conclusion of Theorem 2: The Leading Terms

From the above discussion, we know except for the four nontrivial variables with indices
\[ 10, 20, 30, 40; \quad \text{or} \quad 10, 12, 13, 14; \quad \text{or} \quad 30, 13, 23, 43; \quad \text{or} \quad 40, 14, 24, 34. \]
The contributions from all the other cases are acceptable by the error term in Theorem 2.

Now, if we have indices 10, 20, 30, 40, note in all the cases with respect to the factors of \( a, b, c \), we just need to consider the term in the case
\[ u_s = v_s = w_s = a'_s = b'_s = c'_s = 1, \]
for the contribution of any other case is negligible because of (4.14). Thus
\[ g(\vec{D}) = 4^{-\omega(D)} \sum_{D = D_{10}, D_{20}, D_{30}, D_{40} \geq T} 1, \]

which is easily seen to lead to the contribution

\[ (1 + o(1)) \# S(X; h). \quad (6.1) \]

In the case we have indices 10, 12, 13, 14, the same discussion results in the contribution

\[ (1 + o(1)) \# S(X; h). \quad (6.2) \]

Now for case 30, 13, 23, 43, by (4.14), we have \( u_s = b'_s = c'_s = 1, \ v_s = v, \ w_s = w \) and \( a'_s = a' \); thus, if writing \( D_{ij} = D_i \), we have

\[ g(\vec{D}) = 2^{-\omega(abc)} 4^{-\omega(D)} \sum_{\substack{\gamma(a) = a'u \\ \gamma(b) = b'v \\ \gamma(c) = c'w}} \sum_{D_i \geq T} \left( \frac{vwD_1D_2}{a'D_4} \right) \left( \frac{a'wD_2D_4}{vD_1} \right) \left( \frac{-a'vD_1D_4}{wD_2} \right), \]

the summand of which, from the elementary identity

\[ 1 + \left( \frac{-1}{AB} \right) + \left( \frac{-1}{AC} \right) - \left( \frac{-1}{BC} \right) = 2 \left( \frac{-BC}{A} \right) \left( \frac{AB}{C} \right) \left( \frac{AC}{B} \right), \]

is exactly

\[ \frac{1}{2} \left\{ 1 + \left( \frac{-1}{vwD_1D_2} \right) + \left( \frac{-1}{a'wD_2D_4} \right) - \left( \frac{-1}{-a'vD_1D_4} \right) \right\}. \quad (6.4) \]

The terms involving \( \left( \frac{-1}{x} \right) \) can be dealt with by the estimate of character sums. For example, for the term involving \( \left( \frac{-1}{vwD_1D_2} \right) \), we may take

\[ n_3 = D_1, \quad n_4 = D_4 \]

and, by using lemma 5, attribute its contribution into the error term. Thus, the total contribution in this case is

\[ \left( \frac{1}{2} + o(1) \right) \# S(X; h) \quad (6.5) \]

Similarly, we have the same contribution from the last case. Getting this together with contributions (6.1), (6.2) and (6.5), we have proved theorem 2.

ACKNOWLEDGEMENTS

The author is grateful to Professors Andrew Granville and Carl Pomerance for their helpful comments and encouragement, and to Kevin James for showing the author his PhD thesis.
References


Department of Mathematics, The University of Michigan, 525 E. University Ave., Ann Arbor, MI 48109-1109
E-mail address: gangyu@math.lsa.umich.edu,